EXHIBIT A

2120 - Served
2220 - Not Served
2320 - Served By Mail
2420 - Served By Publication
Summons - Alias Summons

2121 - Served
2221 - Not Served
2321 - Served By Mail
2421 - Served By Publication

(06/28/18) CCG 0001

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS

SHANICE KLOSS, individually and for a class,

(Name all parties)

v.

CASHCRATE, LLC, a Nevada limited liability co.,

Case No. 2018 CH 13520

CSC Services of Nevada, Inc.
2215-B Renaissance Dr.
Las Vegas, NV 89119

☑ **SUMMONS** ☐ **ALIAS SUMMONS**

To each Defendant:

YOU ARE SUMMONED and required to file an answer to the complaint in this case, a copy of which is hereto attached, or otherwise file your appearance and pay the required fee **within thirty (30) days after service of this Summons**, not counting the day of service. To file your answer or appearance you need access to the internet. Please visit www.cookcountyclerkofcourt.org to initiate this process. Kiosks with internet access are available at all Clerk's Office locations. Please refer to the last page of this document for location information.

If you fail to do so, a judgment by default may be entered against you for the relief requested in the complaint.

To the Officer:

This Summons must be returned by the officer or other person to whom it was given for service, with endorsement of service and fees, if any, immediately after service. If service cannot be made, this Summons shall be returned so endorsed. This Summons may not be served later than thirty (30) days after its date.

E-filing is now mandatory for documents in civil cases with limited exemptions. To e-file, you must first create an account with an e-filing service provider. Visit https://efile.illinoiscourts.gov/service-providers.htm to learn more and to select a service provider. If you need additional help or have trouble e-filing, visit http://www.illinoiscourts.gov/FAQ/gethelp.asp.

11/5/2018 1:08 PM DOROTHY BROWN

Witness: _____

DOROTHY BROWN, Clerk of Court

Date of Service: _____
(To be inserted by officer on copy left with Defendant or other person):

Atty. No.: 56618
Atty Name: Jad Sheikali
Atty. for: Plaintiff
Address: 55 West Wacker Drive, 9th Fl.
City: Chicago State: IL
Zip: 60601
Telephone: 312-893-7002
Primary Email: jsheikali@mcgpc.com
Secondary Email: dgerbie@mcgpc.com
Tertiary Email: emeyers@mcgpc.com

CLERK OF THE CIRCUIT COURT OF COOK COUNTY OFFICE LOCATIONS

- Richard J Daley Center
  50 W Washington
  Chicago, IL 60602
- District 2 - Skokie
  5600 Old Orchard Rd
  Skokie, IL 60077
- District 3 - Rolling Meadows
  2121 Euclid
  Rolling Meadows, IL 60008
- District 4 - Maywood
  1500 Maybrook Ave
  Maywood, IL 60153
- District 5 - Bridgeview
  10220 S 76th Ave
  Bridgeview, IL 60455
- District 6 - Markham
  16501 S Kedzie Pkwy
  Markham, IL 60428
- Domestic Violence Court
  555 W Harrison
  Chicago, IL 60607
- Juvenile Center Building
  2245 W Ogden Ave, Rm 13
  Chicago, IL 60602
- Criminal Court Building
  2650 S California Ave, Rm 526
  Chicago, IL 60608

Daley Center Divisions/Departments

- Civil Division
  Richard J Daley Center
  50 W Washington, Rm 601
  Chicago, IL 60602
  Hours: 8:30 am - 4:30 pm
- Chancery Division
  Richard J Daley Center
  50 W Washington, Rm 802
  Chicago, IL 60602
  Hours: 8:30 am - 4:30 pm
- Domestic Relations Division
  Richard J Daley Center
  50 W Washington, Rm 802
  Chicago, IL 60602
  Hours: 8:30 am - 4:30 pm
- Civil Appeals
  Richard J Daley Center
  50 W Washington, Rm 801
  Chicago, IL 60602
  Hours: 8:30 am - 4:30 pm
- Criminal Department
  Richard J Daley Center
  50 W Washington, Rm 1006
  Chicago, IL 60602
  Hours: 8:30 am - 4:30 pm
- County Division
  Richard J Daley Center
  50 W Washington, Rm 1202
  Chicago, IL 60602
  Hours: 8:30 am - 4:30 pm
- Probate Division
  Richard J Daley Center
  50 W Washington, Rm 1202
  Chicago, IL 60602
  Hours: 8:30 am - 4:30 pm
- Law Division
  Richard J Daley Center
  50 W Washington, Rm 801
  Chicago, IL 60602
  Hours: 8:30 am - 4:30 pm
- Traffic Division
  Richard J Daley Center
  50 W Washington, Lower Level
  Chicago, IL 60602
  Hours: 8:30 am - 4:30 pm

12-Person Jury

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

SHANICE KLOSS, individually and on behalf of similarly situated individuals, *Plaintiff,* v. CASHCRATE, LLC, a Nevada limited liability company, *Defendant.*	)	No. 2018CH13520 Hon. **Jury Demanded**

CLASS ACTION COMPLAINT & JURY DEMAND

Plaintiff, Shanice Kloss ("Plaintiff"), individually and on behalf of a class of similarly situated persons, brings this Class Action Complaint against Defendant CASHCRATE, LLC ("Defendant" or "CashCrate"), as a result of its conduct concerning a data breach ("Data Breach" or "Data Hack") that compromised private personal information of the Plaintiff and millions of other members of the putative class due to Defendant's failure to implement a reasonably adequate cybersecurity prevention, detection, and response protocol. Plaintiff alleges as follows based on personal knowledge as to her own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by her attorneys.

INTRODUCTION

1. On or before November, 2016, CashCrate was the target of a Data Hack on its information technology ("IT") systems.

2. This Data Breach resulted in unauthorized outside parties gaining access to CashCrates's customers' sensitive and confidential personal information, including their names, home and business addresses, email addresses, demographic information, and passwords ("PII"). Even though CashCrate was storing sensitive information that it knew was of value to, and

vulnerable to, cyber attackers, CashCrate failed to take basic security precautions that could have prevented the disclosure of its customers' PII.

3. CashCrate's lax cybersecurity procedures allowed hackers to obtain access to Plaintiff's and other customers' PII. This PII should have been secured by adequate levels of protection and should not have been susceptible to unauthorized access.

4. After accessing CashCrate's IT systems, hackers were able to extract the PII for over six million (6,000,000) CashCrate account holders.

5. To this day, Defendant has failed to notify Plaintiff that her PII was compromised in the Data Breach. On information and belief, Defendant has failed to implement any reasonable breach notification process following the Data Breach.

PARTIES

6. Defendant CashCrate, is a Nevada Limited Liability Company that is transacting business in Cook County, Illinois and maintains its headquarters in Nevada. Defendant CashCrate transacts, and intentionally seeks to transact, business with Illinois residents.

7. At all relevant times, Plaintiff Shanice Kloss has been a resident and citizen of the State of Illinois.

JURISDICTION AND VENUE

8. This Court may assert personal jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 in accordance with the Illinois Constitution and the Constitution of the United States because Defendant is doing business within this State and because Plaintiff's claims arise out of Defendant's unlawful in-state actions, as Plaintiff used Defendant's services in Illinois, and Defendant failed to take reasonable precautions to guard against, respond to, and detect cyberattacks in this State.

9. Venue is proper in Cook County pursuant to 735 ILCS 5/2-101, because Defendant is doing business in Cook County and, thus, resides there under § 2-102, and because Plaintiff used the cash-for-survey's services from Defendant in Cook County.

FACTS SPECIFIC TO PLAINTIFF

10. On or around November 2016, Defendant was the target of a Data Hack when third-party hackers were able to gain access to its IT systems. Defendant was not able to prevent, thwart, or reasonably detect the Data Hack, resulting in exposure of the PII of over six million (6,000,000) of its customers to criminals. The hackers simultaneously released the PII of these millions of customers to the public domain. The Data Hack resulted in the shutdown of CashCrates's IT systems.

11. Defendant's inadequate technical and administrative cybersecurity protocols resulted in an unreasonable delay in detecting the Data Hack for several months, thereby greatly aggravating the damages incurred by Plaintiff.

12. The PII exposed as a result of Defendant's cybersecurity practices includes not only name, account, and demographic information, but also easily-accessible password information. Because Defendant failed to implement reasonable technical safeguards, including adequate encryption technology, the password data, once obtained and released by the hackers, was easily decrypted by the subject hackers.

13. Despite the severity of the Data Breach, CashCrate failed to conduct a reasonable breach notification protocol. Aside from a passive support page, CashCrate failed to take measures to alert Plaintiff that her PII had been compromised in the Data Breach or otherwise engage in a campaign of directly notifying affected customers within a reasonable timeframe.

14. It was not until September 2018 did Plaintiff learn of the Data Breach through her own investigation and efforts.

15. Defendant's failure to implement a reasonable cybersecurity protocol that included adequate technical, administrative, and physical controls allowed the hackers to access its IT system, and ultimately, directly access Plaintiff's and other customers' PII, including passwords. For example, an adequate intrusion detection and prevention system would have alerted CashCrate to the presence of hackers, administrative controls would have prepared CashCrate's staff to detect irregularities in the IT system, and technical measures such as adequate encryption that was not readily-crackable would have prevented access to hashed password values.

16. Notably, Defendant not only failed to protect Plaintiff's and other customers' PII, but also failed to inform them of the Data Breach in a reasonable manner and without undue delay. Without identifying any justification, and in violation of the law, Defendant failed to promptly and adequately notify Plaintiff of the Data Breach.

17. Given the current prevalence of cybersecurity awareness, especially in light of constant, high profile data breaches, Defendant knew of the risks inherent in capturing, storing, and using the PII of its customers and the consequences of the exposure of such PII to unauthorized third parties, as well as the importance of promptly notifying affected parties in the event of a breach incident.

18. Had Defendant informed Plaintiff of the Data Breach within a reasonable period of time as required by law and/or through a reasonable manner and medium, Plaintiff and the other members of the putative class would have been able to take actions to protect their identities, accounts, and other potential targets from further misuse. Instead Defendant let its customers

languish in ignorance as to the real risk of irreversible privacy harms presented by the unauthorized parties who had gained access to their PII.

19. Plaintiff believed that Defendant would take reasonable measures to secure her PII. Had Plaintiff known that Defendant would fail to take reasonable safeguards to protect and secure her PII, she would not have utilized Defendant's commercial services, or she would have at least acted differently upon weighing the risk in having her PII left vulnerable to attack.

20. Defendant's failure to comply with reasonable data security standards provided Defendant a benefit in the form of saving on the costs of compliance, but at the expense and severe detriment of Defendant's own customers, including Plaintiff, whose PII has been exposed in the Data Breach and placed at serious and ongoing risk of imminent misuse and identity theft.

21. Since recently becoming aware of the Data Breach, Plaintiff has taken time and effort to mitigate her risk of identity theft, including monitoring her credit and financial accounts.

22. Plaintiff has also been harmed by having her PII compromised and faces the imminent and impending threat of future additional harm from the increased threat of identity theft and fraud due to her PII being sold, misappropriated, or otherwise misused by unknown parties. Indeed, Plaintiff has suffered substantive privacy and informational injuries.

23. Plaintiff has also experienced mental anguish as a result of the Data Breach. She experiences anxiety and anguish when thinking about what would happen if her identity is stolen as a result of the Data Breach; when wondering how long and to how many parties her PII was exposed before the Data Breach was even discovered by Defendant; and when she thinks about the fact that Defendant was aware of the Data Breach and actively decided to keep her and the other victims of the Data Breach ignorant of the fact that their PII had been compromised.

24. The Data Breach was caused and enabled by Defendant's knowing violation of its obligations to abide by adequate practices and industry standards in protecting customers' PII. CashCrate wholly failed to comply with reasonable cybersecurity standards and allowed its customers' PII to be compromised, all in an effort to save money by cutting corners on security measures that could have prevented or mitigated the Data Breach.

25. Defendant also avoided the cost of notifying, individually, over 6,000,000 of its customers, including the Plaintiff herself.

CLASS ALLEGATIONS

26. Plaintiff brings Counts I through IV, as set forth below, on behalf of herself and a Class and Subclass (together, the "Class") of similarly situated individuals pursuant to 735 ILCS § 5/2-801. The Class and Subclass are defined as follows:

> **Class:** All persons whose Personal Information was in the possession of Defendant, or any of its subsidiaries, at any point during the Data Breach.
>
> **Illinois Subclass:** All Illinois residents whose Personal Information was in the possession of Defendant, or any of its subsidiaries, at any point during the Data Breach.

27. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendant; and any immediate family member of such officer or director.

28. Upon information and belief, there are millions of members of the Class, making the members of the Class so numerous that joinder of all members is impracticable. Although the exact number of Class is currently unknown, it is believed to be over six million (6,000,000) and can easily be ascertained through Defendant's records.

29. Plaintiff's claims are typical of the claims of the Class members she seeks to represent because the factual and legal bases of Defendant's liability to Plaintiff and the other

Class members are the same and because Defendant's conduct has resulted in similar injuries to Plaintiff and to the Class members. As alleged herein, Plaintiff and the other Class members have all suffered damages as a result of Defendant's failure to maintain reasonable security safeguards with respect to its handling and storage of customers' sensitive PII.

30. There are many questions of law and fact common to the claims of Plaintiff and the other Class members, and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendant adequately safeguarded Plaintiff and the Class members' PII;

b. Whether Plaintiff and the Class members were notified of the Data Breach within a reasonable period of time and through a reasonable method;

c. Whether Defendant willfully, recklessly, and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class members' PII;

d. Whether there was an unauthorized disclosure of the Class members' PII;

e. Whether implied or express contracts existed between Defendant and the Class members;

f. Whether Plaintiff and the Class members sustained damages as a result of Defendant's failure to adequately safeguard their PII;

g. Whether Defendant's PII storage and protection protocols and procedures were reasonable under industry standards;

h. Whether Defendant's cybersecurity prevention, detection, and notification protocols were reasonable under industry standards;

i. Whether Defendant misrepresented the safety and security of the Class members' PII maintained by Defendant;

j. When Defendant became aware of the unauthorized access to Plaintiff's and the Class members' PII;

k. Whether Defendant's conduct violated the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*; and

31. Absent a class action, most Class members would find the cost of litigating their claims to be prohibitively expensive and would have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

32. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class she seeks to represent. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the other Class members and have the financial resources to do so. Neither Plaintiff nor her counsel has any interest adverse to those of the other members of the Class.

33. Defendant has acted and failed to act on grounds generally applicable to the Plaintiff and the other Class members, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

COUNT I
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*
(On behalf of Plaintiff and the Illinois Subclass)

34. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

35. Pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq.*, Defendant was required to implement and maintain reasonable security measures to protect the Plaintiff's and Illinois Subclass members' PII, and to notify them regarding any unauthorized disclosure in the most expedient time possible and without unreasonable delay.

36. Defendant's unlawful conduct alleged herein in failing to safeguard its customers' PII, and subsequent failure to timely notify its customers that such PII had been compromised, constitute violations of the Illinois Personal Information Protection Act.

37. Pursuant to Section 530/20 of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.* ("ICFA"), a violation of the Illinois Personal Information Protection Act, as alleged herein, is itself deemed an "unlawful practice" and violation under the ICFA, and Defendant has therefore violated the ICFA.

38. Plaintiff and the Illinois Subclass members have suffered injury in fact and actual damages, as alleged herein, as a result of Defendant's unlawful conduct and violations of the ICFA.

39. Wherefore, Plaintiff prays for relief as set forth below.

COUNT II
Breach of Contract
(On behalf of Plaintiff and the Class)

40. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

41. Plaintiff and the Class members are parties to express agreements with Defendant whereby Plaintiff and the Class members provide their PII to Defendant in exchange for reward-for-survey services from Defendant, including the provision of reasonable safeguards to prevent the unauthorized disclosure of PII. Defendant's business model depends on the extraction of data from customers, so it should have been incumbent on Defendant to engage in reasonable cybersecurity practices.

42. Defendant's failure to implement an adequate and reasonable data privacy and cybersecurity protocol which included adequate prevention, detection, and notification procedures constitutes a breach of contract.

43. Plaintiff and the Class members would not have provided and entrusted their PII to Defendant in the absence of an agreement with Defendant to reasonably safeguard their PII and to reasonably notify them of unauthorized disclosures.

44. Plaintiff and the members of the Class fully performed their obligations under their contracts with Defendant.

45. Defendant breached the contracts it made with Plaintiff and the Class members by failing to safeguard and protect their PII, and by failing to notify them in a timely and accurate manner that that their PII was compromised as a result of the Data Breach.

46. The damages expressed herein as sustained by Plaintiff and the Class members were the direct and proximate result of Defendant's breaches of contract.

47. Wherefore Plaintiff prays for the relief set forth below.

COUNT III
Breach of Implied Contract
(On behalf of Plaintiff and the Class) (in the alternative to Count II)

48. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

49. Plaintiff and the Class members were required to provide Defendant their PII as a condition of using Defendant's services for filling out surveys for money. To the extent that it is found that Defendant did not have an express contract with Plaintiff and the Class members, Defendant entered into implied contracts with Plaintiff and the Class members whereby, by virtue of such requirement to provide their PII, Plaintiff and the Class members and Defendant entered into implied contracts whereby Defendant was obligated to take reasonable steps to secure and safeguard such PII and obligated to take reasonable steps following an unauthorized disclosure of the same.

50. Defendant's failure to implement an adequate and reasonable data privacy and cybersecurity protocol which included adequate prevention, detection, and notification procedures constitutes a breach of an implied contract between Defendant and the Class members.

51. Plaintiff and the Class Members would not have provided and entrusted their PII to Defendant in order to use the cash-for-money surveys from Defendant, and certainly not at the offered rate for such services, in the absence of an agreement with Defendant to reasonably safeguard their PII and to reasonably notify them of unauthorized disclosures

52. Plaintiff and the members of the Class fully performed their obligations under their implied contracts with Defendant.

53. Defendant breached the implied contracts it made with Plaintiff and the Class members by failing to safeguard and protect their PII, and by failing to notify them in a timely and accurate manner that that their PII was compromised as a result of the Data Breach.

54. The damages expressed herein as sustained by Plaintiff and the Class members were the direct and proximate result of Defendant's breaches of contract.

55. Wherefore Plaintiff prays for the relief set forth below.

COUNT IV
Negligence
(On behalf of Plaintiff and the Class)

56. Plaintiff realleges and incorporates by reference the foregoing allegations as if fully set forth herein.

57. As a condition of using its services, Defendant required Plaintiff and Class members to provide their PII.

58. At all relevant times, Defendant had a duty, or assumed a duty, to implement reasonable data privacy and cybersecurity protocol, including adequate prevention, detection, and

notification procedures, in order to safeguard the PII of the Plaintiff and the Class members and to prevent the unauthorized access to and disclosures of the same.

59. A duty was also created due to the special relationship between Defendant, as the entity with all knowledge and control regarding relevant and material facts concerning the nature in which PII is stored, maintained, and secured, and Plaintiff, as a customer of Defendant who was required to provide her PII in order to use Defendant's marketed services.

60. Defendant breached the aforementioned duty in, including but not limited to, one or more of the following ways:

a. Failing to implement reasonable data privacy and cybersecurity measures to secure its or Plaintiff's and Class members' email accounts, including failing to require adequate multifactor authentication and encryption;

b. Failing to implement a reasonable data privacy and cybersecurity protocol, including adequate procedures for preventing cybersecurity threats and/or detecting such threats in a timely manner;

c. Failing to notify Plaintiff and Class member's that their PII had been disclosed to nefarious hackers within a reasonable period of time and/or through a reasonable manner or method;

d. Failing to reasonably comply with applicable state and federal law concerning its data privacy and cybersecurity protocol, including the substance and manner of its unreasonably-delayed notification to Plaintiff and Class members concerning the Data Breach; and

e. Otherwise failing to act reasonably under the circumstances and being negligent with regards to its conduct in preventing, detecting, and disclosing the subject Data Breach.

61. Defendant knew, or should have known, that its data privacy and cybersecurity protocol failed to reasonably protect Plaintiff and the Class members' PII.

62. As a direct result of Defendant's aforesaid negligent acts and omissions, Plaintiff and the Class members suffered injury and damages, including the loss of their legally protected interest in the confidentiality and privacy of their PII, the loss of the benefit of their bargain in

completing survey's from Defendant, pecuniary injury in the form of time and expense to mitigate the disclosure and/or significantly increased risk of exposure of PII to nefarious third parties.

63. Wherefore Plaintiff prays for the relief set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class and Subclass set forth above, respectfully requests the Court order relief and enter judgement against Defendant:

A. Certifying the Class and Subclass identified above and appointing Plaintiff as Class representative and the undersigned counsel as Class counsel;

B. Awarding Plaintiff and the Class and Subclass appropriate relief, including actual, statutory, compensatory, and/or punitive damages;

C. Requiring Defendant to furnish identity fraud monitoring and mitigation services for a reasonable period of time;

D. Granting injunctive relief requiring Defendant to implement commercially reasonable security measures to properly guard against any and all future cyberattacks and to provide prompt, reasonable notification in the event of such an attack;

E. Requiring Defendant to pay Plaintiff's and the Class members' reasonable attorneys' fees, expenses, and costs; and

F. Any such further relief as this Court deems reasonable and just.

DEMAND FOR TRIAL BY JURY

Plaintiff demands a trial by jury on all issues so triable.

Dated: October 30, 2018

Respectfully submitted:

SHANICE KLOSS, individually and on behalf of a class of similarly situated individuals

By: /s/ Jad Sheikali
One of Plaintiff's Attorneys

Jad Sheikali
William Kingston
McGUIRE LAW, P.C. (Firm ID 56618)
55 W. Wacker Dr., 9th Fl.
Chicago, IL 60601Tel:
(312) 893-7002
jsheikali@mcgpc.com
wkingston@mcgpc.com

Attorneys for Plaintiff and the Putative Classes